数理解析研究所講究録 1319 巻 2003 年 139-147

On a distribution property of the residual order of $a(\mathrm{mod}\ p)$, III

Leo Murata* and Koji Chinen†

村田　玲音 (明治学院大学　経済学部)
知念　宏司 (大阪工業大学　工学部)

1 Introduction

Let $\mathbf{N}$ be the set of all natural numbers, $\mathbf{P}$ the set of all prime numbers. And p always denotes a prime number, $\pi(x)$ the number of primes not exeeding x.

For a fixed natural number $a\geq 2$, we can define two functions, I_a and D_a, from $\mathbf{P}$ to $\mathbf{N}$:

$$\begin{aligned} I_a: \ p \ &\mapsto \ I_a(p)=|(\mathbf{Z}/p\mathbf{Z})^{\times}:\langle a \pmod p\rangle| \\ &\qquad \text{(the residual index of } a \text{ (mod } p)), \\ D_a: \ p \ &\mapsto \ D_a(p)=\sharp\langle a \pmod p\rangle \\ &\qquad \text{(the residual order of } a \text{ (mod } p) \text{ in } (\mathbf{Z}/p\mathbf{Z})^{\times}), \end{aligned}$$

where $(\mathbf{Z}/p\mathbf{Z})^{\times}$ denotes the set of all invertible residue classes modulo p, and $|\ :\ |$ the index of the subset.

We have a simple relation

$$I_a(p)\ D_a(p)=p-1,$$

but both of these functions fluctuate quite irregularly. More than 200 years ago, C. F. Gauss calculated these numbers and he already noticed that

(a) The movement of I_{10} is much more modest than D_{10},
(b) $I_{10}(p)=1$ happens rather frequently.

*Department of Mathematics, Faculty of Economics, Meiji Gakuin University, 1-2-37 Shirokanedai, Minato-ku, Tokyo 108-8636, Japan. E-mail: leo@eco.meijigakuin.ac.jp

†Department of Mathematics, Faculty of Engineering, Osaka Institute of Technology. Omiya, Asahi-ku, Osaka 535-8585, Japan. E-mail: YHK03302@nifty.ne.jp

So he studied only about the distribution property of $I_a(p)$ and conjectured that

$$\sharp\{p \in \mathbf{P} \ : I_{10}(p) = 1\} = \infty,$$

which is now a part of so-called **Artin's conjecture for primitive root.**

Let us define the set, for a natural number n,

$$N_a(x; n) = \{p \leq x \ ; \ I_a(p) = n\},$$

then we already knows that

Theorem A ([5],[6]) *We assume the Generalized Riemann Hypothesis(GRH). Then*

$$\sharp N_a(x; n) = C_a^n \ \pi(x) + O\left(\frac{x \log\log x}{\log^2 x}\right),$$

where C_a^n is a computable constant depends only on a and n.

and

Corollary 1 *We assume GRH. When a is square-free and $a \not\equiv 1 \pmod 4$, the map I_a is surjective from* $\mathbf{P}$ *to* $\mathbf{N}$.

And on the map D_a, we have

Theorem B *The map D_a is almost surjective from* $\mathbf{P}$ *to* $\mathbf{N}$.

Where "almost surjective" means "except for only finite members of n's".

But we notice a big difference between these two surjectivities. For any $n \in \mathbf{N}$, the set

$$D_a^{-1}(\{n\}) = \{p \in \mathbf{P} \ ; \ D_a(p) = n\}$$

contains only a finite number of elements. In fact, if $D_a(p) = n$, then

$$n + 1 \leq p \leq a^n.$$

On the contrary, Theorem A shows that (under GRH),

$$I_a^{-1}(\{n\}) = \{p \in \mathbf{P} \ ; \ I_a(p) = n\} \sim C_a^{(n)} \text{ times of } \mathbf{P}.$$

So, the map $I_a(p)$ covers $\mathbf{N}$ very *thickly*, while the map $D_a(p)$ covers $\mathbf{N}$ very *thinly*.

Here we want to study distribution properties of $D_a(p)$. Then taking into account of the above facts, we think we should take a subset $\mathbf{S}$ of $\mathbf{N}$ which contains *infinitely* many elements, and consider the inverse image

$$D_a^{-1}(\mathbf{S}) = \{p \leq x \ ; \ D_a(p) \in \mathbf{S}\}.$$

In this note, in Section 2 we take $\mathbf{S} = \{$a residue class in $\mathbf{N}\}$ (joint work of K. Chinen and L. Murata), and in Section 3 we take $\mathbf{S} = \mathbf{P}$ (joint work of C. Pomerance and L. Murata).

2 The case S = a residue class in N

This part is a sequel of our previous works [1],[2]. See also [3],[7].

2.1 A residue class mod 4

Let us take **S** as a residue class mod 4. Namely we define, for $l = 0, 1, 2, 3$,

$$Q_a(x; 4, l) = \{p \le x \; ; \; D_a(p) \equiv l \pmod 4\}.$$

Then, in our previous paper, we proved

Theorem 1 ([7]) *We assume $a \in \mathbf{N}$ is not a perfect h-th power with $h \ge 2$, and put*

$$a = a_1 a_2^2, \quad a_1 : \textit{ square free.}$$

When $a_1 \equiv 2 \pmod 4$, we define a_1' by

$$a_1 = 2a_1'.$$

We assume GRH. And we define an absolute constant C by

$$C = \prod_{p \equiv 3 \pmod 4} \left(1 - \frac{2p}{(p^2+1)(p-1)}\right).$$

Then, for $l = 1, 3$, we have an asymptotic formula

$$\sharp Q_a(x; 4, l) = \delta_l \; \pi(x) + O\left(\frac{x}{\log x \log\log x}\right),$$

and the leading coefficients (=the natural density) δ_l $(l = 1, 3)$ are given by the following way:

(I) *If $a_1 \equiv 1, 3 \pmod 4$, then $\delta_1 = \delta_3 = \dfrac{1}{6}$.*

(II) *When $a_1 \equiv 2 \pmod 4$,*

(i) *If $a_1' = 1$, i.e. $a = 2 \cdot$ (a square number), then*

$$\delta_1 = \frac{7}{48} - \frac{C}{8}, \quad \delta_3 = \frac{7}{48} + \frac{C}{8}.$$

(ii) *If $a_1' \equiv 1 \pmod 4$ with $a_1' > 1$, then*

(ii-1) *if a_1' has a prime divisor q with $q \equiv 1 \pmod 4$, then $\delta_1 = \delta_3 = \dfrac{1}{6}$,* (ii-2) *if all prime divisors* q *of* a_1' *satisfy* $q \equiv 3 \pmod 4$, *then*

$$\begin{aligned}
\delta_1 &= \frac{1}{6} - \frac{C}{8}\prod_{p \mid a_1'}\left(\frac{-2p}{p^3-p^2-p-1}\right),\\
\delta_3 &= \frac{1}{6} + \frac{C}{8}\prod_{p \mid a_1'}\left(\frac{-2p}{p^3-p^2-p-1}\right).
\end{aligned}$$

(iii) *If* $a_1' \equiv 3 \pmod 4$, *then*

(iii-1) *if* a_1' *has a prime divisor* q *with* $q \equiv 1 \pmod 4$, *then* $\delta_1 = \delta_3 = \dfrac{1}{6}$,

(iii-2) *if all prime divisors* q *of* a_1' *satisfy* $q \equiv 3 \pmod 4$, *then*

$$\begin{aligned}
\delta_1 &= \frac{1}{6} + \frac{C}{8}\prod_{p \mid a_1'}\left(\frac{-2p}{p^3-p^2-p-1}\right),\\
\delta_3 &= \frac{1}{6} - \frac{C}{8}\prod_{p \mid a_1'}\left(\frac{-2p}{p^3-p^2-p-1}\right).
\end{aligned}$$

This theorem shows that, roughly speaking, *usually* we have rather *beautiful* distribution

$$\begin{array}{lllll}
 & \sharp Q_a(x;4,0) & \sim \frac{1}{3}\,\pi(x) & \longleftarrow & \text{unconditional}\\
 & \sharp Q_a(x;4,1) & \sim \frac{1}{6}\,\pi(x) & & \\
\pi(x) & & & & \\
 & \sharp Q_a(x;4,2) & \sim \frac{1}{3}\,\pi(x) & & \\
 & \sharp Q_a(x;4,3) & \sim \frac{1}{6}\,\pi(x) & \longleftarrow & \text{we need GRH}
\end{array}$$

And we notice that when $(a_1, 4) > 1$ the distribution turns into a little *irregular* one. Anyway it seems an interesting phenomenon, in II-(ii) and II-(iii), the densities δ_1 and δ_3 are controled by whether a_1' has a prime factor q with $q \equiv 1 \pmod 4$ or not.

For numerical examples, see Section 4, Table 4.1 - Table 4.3.

Then, what happens for another modulus?

2.2 A residue class mod 5

We can not find a good probabilistic model for this problem so far, i.e. we do not know why the natural density of $Q_a(x;4,1)$ should be equal to $\frac{1}{6}$?

But here we remark that this problem has a relation to the structure of the additive group $\mathbf{Z}/4\mathbf{Z}$.

$$\begin{array}{ccc}
\mathbf{Z}/4\mathbf{Z} = \{\bar{0},\bar{1},\bar{2},\bar{3}\} & \longleftrightarrow & \sharp Q_a(x;4,\mathbf{Z}/4\mathbf{Z}) \sim \pi(x) \\
\cup & & \\
\{\bar{0},\bar{2}\} & \longleftrightarrow & \sharp Q_a(x;4,\bar{0}\cup\bar{2}) \sim \frac{2}{3}\pi(x) \\
\cup & & \\
\{\bar{0}\} & \longleftrightarrow & \sharp Q_a(x;4,\bar{0}) \sim \frac{1}{3}\pi(x)
\end{array}$$

And in order to separate $\bar{1}$ and $\bar{3}$, we need GRH.

Then, since $\mathbf{Z}/5\mathbf{Z} = \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\}$ has only one additive subgroup $\{\bar{0}\}$, we can expect that we can get an asymptotic formula for $\sharp Q_a(x;5,\bar{0})$ and we need GRH to get an asymtpotic formula for $\sharp Q_a(x;4,\bar{j})$ for $j = 1,2,3,4$. And it is true.

Here we show our result only some simple cases. Namely we assume $a \in \mathbf{N}$ is not a perfect h-th power with $h \geq 2$, and put

$$a = a_1 a_2^2, \quad a_1 : \text{ square free,}$$

as above, and further assume $5 \nmid a_1$ — as we remarked already, when $5|a_1$, we have rather irregular densities.

Theorem 2 *Let G be the multiplicative group of all characters modulo 5. We define, for $\chi \in G$, the numbers β_χ and C_χ by*

$$\beta_\chi = \begin{cases} 1, & \chi \in G^2, \\ -1, & \textit{otherwise}, \end{cases}$$

and

$$C_\chi = \prod_{p \neq 5} \frac{p^3 - p^2 - p + \chi(p)}{(p-1)(p^2 - \chi(p))}.$$

(I) *If $j = 0$, then we have an asymptotic formula unconditionally*

$$\sharp Q_a(x;5,0) = \frac{5}{24}\,\pi(x) + O\left(\frac{x}{\log x \log\log x}\right).$$

(II) *When $j \neq 0$, we assume GRH. Then we have*

$$\sharp Q_a(x;5,j) = \delta_j\,\pi(x) + O\left(\frac{x}{\log x \log\log x}\right),$$

and the leading coefficient is given by

(II-1) *If $a_1 \equiv 1 \pmod 4$, then*

$$\delta_j = \frac{25}{96} - \frac{1}{16}\sum_{\chi \in G} \beta_\chi\, \chi(j)\, C_\chi \left(1 + \prod_{p|2a_1} \frac{p\,(\chi(p)-1)}{p^3 - p^2 - p + \chi(p)}\right).$$

(II-2) *If* $a_1 \equiv 2 \pmod 4$, *then*

$$\delta_j = \frac{25}{96} - \frac{1}{16}\sum_{\chi\in G}\beta_\chi\ \chi(j)\ C_\chi\left(1+\frac{\chi(2)^2}{16}\prod_{p|2a_1}\frac{p\ (\chi(p)-1)}{p^3-p^2-p+\chi(p)}\right).$$

(II-3) *If* $a_1 \equiv 3 \pmod 4$, *then*

$$\delta_j = \frac{25}{96} - \frac{1}{16}\sum_{\chi\in G}\beta_\chi\ \chi(j)\ C_\chi\left(1+\frac{\chi(2)}{4}\prod_{p|2a_1}\frac{p\ (\chi(p)-1)}{p^3-p^2-p+\chi(p)}\right).$$

We can prove this theorem by the similar method which we used in [7], but in order to separate four classes — $\bar{1}, \bar{2}, \bar{3}, \bar{4}$ — we need Dirichlet characters and very complicated calculations.

We can extend this result to much more general moduli, such as q^r with a prime q (see [4]).

For $\chi \notin G^2$, the number C_χ is *not a real number*. The most interesting feature of this result may be the fact that a combination of these complex numbers gives the *real* density of $\sharp Q_a(x; 5, j)$.

For numerical examples, see Section 4, Table 4.4 - Table 4.6.

3 The case $S = \mathbf{P}$

Here we take $a = 2$, and consider the set

$$M(x) = \{p \le x\ ;\ I_2(p) \text{ is prime}\}.$$

On the cardinality of this set, Pomerance [9] proved

Theorem C *We have unconditionaly*

$$\sharp M(x) \ll \pi(x)\frac{\log\log\log x}{\log\log x},$$

and under GRH,

$$\sharp M(x) \ll \pi(x)\frac{\log\log x}{\log x}.$$

We can improve the latter estimate as follows :

Theorem 3 ([8]) *We assume GRH. Then we have*

$$\sharp M(x) \ll \pi(x)\frac{1}{\log x}.$$

Here we remark that, this estimate seems to be *best possible.* In fact, let us consider the set

$$L(x) = \{p \leq x \ ; \ \frac{p-1}{2} \text{ is also prime, } p \equiv 7 \ (\text{mod}8)\}.$$

Then, it is easy to see that $L(x) \subset M(x)$, and it is (not yet proved but) conjectured that

$$\sharp L(x) \sim C \ \pi(x) \frac{1}{\log x}$$

with a strictly positive constant C, which gives a lower bound of $\sharp M(x)$.

For the proof, see [8].

4 Some numerical examples

Here we show some numerical examples to compare our theoretical results with experimental results.

In the Tables 4.1 - 4.3, we compare the theoretical densities and the experimental densities $\pi(x)^{-1}\sharp Q_a(x;4,j)$ for $x = 10^3, 10^4, 10^5, 10^6, 10^7$.

Table 4.1. The densities of $Q_5(x;4,l)$

Theoretical densities are typical $\left(\frac{1}{3}, \frac{1}{6}, \frac{1}{3}, \frac{1}{6}\right)$.

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.319277	0.156627	0.349398	0.174699
10^4	0.327628	0.167074	0.340668	0.164629
10^5	0.334619	0.167049	0.333055	0.165276
10^6	0.333227	0.167155	0.332934	0.166684
10^7	0.333320	0.166771	0.333099	0.166810

Table 4.2. The densities of $Q_{50}(x;4,l)$

Theoretical densities are $\left(\frac{5}{12}, \frac{7}{48} - \frac{C}{8} \approx 0.06538, \frac{7}{24}, \frac{7}{48} + \frac{C}{8} \approx 0.22629\right)$.

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.415663	0.036145	0.295181	0.253012
10^4	0.409943	0.068460	0.290139	0.231459
10^5	0.416684	0.065172	0.292284	0.225860
10^6	0.416569	0.065889	0.291633	0.225910
10^7	0.416719	0.065351	0.291584	0.226345

Table 4.3. The densities of $Q_6(x;4,l)$

Theoretical densities are $\left(\frac{1}{3}, \frac{1}{6} - \frac{3C}{56} \approx 0.13219, \frac{1}{3}, \frac{1}{6} + \frac{3C}{56} \approx 0.20115\right)$.

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.331325	0.126506	0.325301	0.216867
10^4	0.334963	0.133659	0.333333	0.198044
10^5	0.333785	0.133577	0.332847	0.199791
10^6	0.333151	0.132249	0.333507	0.201093
10^7	0.333331	0.132179	0.333019	0.201471

Here are some examples where the modulus is 5. In the following tables, the second row shows the theoretical density.

Table 4.4. The densities of $Q_{21}(x;5,l)$

x	$l=0$	$l=1$	$l=2$	$l=3$	$l=4$
	0.208333	0.235494	0.176925	0.233715	0.145532
10^3	0.193939	0.266667	0.163636	0.260606	0.120482
10^4	0.209625	0.242251	0.166395	0.235726	0.145069
10^5	0.210554	0.242048	0.174054	0.230160	0.147862
10^6	0.208179	0.236091	0.176457	0.233251	0.143472
10^7	0.208218	0.236068	0.176878	0.233708	0.144110

Table 4.5. The densities of $Q_6(x;5,l)$

x	$l=0$	$l=1$	$l=2$	$l=3$	$l=4$
	0.208333	0.233302	0.179043	0.234686	0.144636
10^3	0.204819	0.289157	0.192771	0.198795	0.114458
10^4	0.215974	0.246944	0.175224	0.231459	0.130399
10^5	0.208133	0.231283	0.181335	0.231178	0.148071
10^6	0.208571	0.232840	0.179219	0.235362	0.144007
10^7	0.208645	0.233330	0.179161	0.234770	0.144093

Table 4.6. The densities of $Q_3(x;5,l)$

x	$l=0$	$l=1$	$l=2$	$l=3$	$l=4$
	0.208333	0.238076	0.169818	0.235252	0.148521
10^3	0.210843	0.210843	0.186747	0.259036	0.132530
10^4	0.211084	0.238794	0.160554	0.234719	0.154849
10^5	0.208238	0.241397	0.164964	0.235036	0.150365
10^6	0.208125	0.238687	0.169448	0.234725	0.149014
10^7	0.208340	0.238100	0.169499	0.235312	0.148749

References

[1] Chinen, K. and Murata, L : On a distribution property of the residual orders of a (mod p) (in Japanese) in *Analytic Number Theory — Expectations for the 21st Century —*, RIMS Kokyuroku **1219** (2001), 245-255.

[2] Chinen, K. and Murata, L : On a distribution property of the residual orders of a (mod p), II (in Japanese) in *New Aspects of Analytic Number Theory*, RIMS Kokyuroku **1274** (2002), 62-69.

[3] Chinen, K. and Murata, L : On a distribution property of the residual order of a (mod p), (preprint). (e-print archive, http://xxx.lanl.gov/archive/math, article number — math. NT/0211077)

[4] Chinen, K. and Murata, L : On a distribution property of the residual orders of a (mod p), III. (preprint).

[5] Lenstra Jr., H. W. : On Artin's conjecture and Euclid's algorithm in global fields, Invent. Math. **42** (1977), 201-224.

[6] Murata, L. : A problem analogous to Artin's conjecture for primitive roots and its applications, Arch. Math. **57** (1991), 555-565.

[7] Murata, L and Chinen, K : On a distribution property of the residual orders of a (mod p), II. (preprint). (e-print archive, http://xxx.lanl.gov/archive/math, article number — math. NT/0211083)

[8] Murata, L and Pomerance, C : On the largest prime factor of a Mersenne number, (preprint).

[9] Pomerance, C : On primitive divisors of Mersenne numbers, Acta Arith. **46** (1986), 355-367.